Journal of Pure and Applied Algebra 13 (1978) 165–168.

A PRESENTATION OF THE SYMMETRIC GROUP BASED ON UNIQUE IRREDUNDANT NONDECREASING FACTORIZATION

William CRAIG

University of California, Berkeley, CA 94720, USA

Communicated by P. Freyd
Received summer 1977

For an arbitrary integer $n \geq 2$ we shall consider the symmetric group S_n whose elements are the $n!$ permutations of $\{1, \ldots, n\}$. We let $i, j, \ldots$ range over $\{1, \ldots, n\}$. For each i we let i be the cyclic permutation $(1, \ldots, i)$ of $\{1, \ldots, n\}$. Thus when $m < i$ then $i(m) = m+1$, when $m = i$ then $i(m) = 1$, and when $m > i$ then $i(m) = m$. A *word* shall be a finite nonempty sequence each term of which is either some i or some i^{-1}. To each word there *corresponds* in an obvious way a unique element of S_n. For example, to ik there corresponds the π in S_n which for each m satisfies $\pi(m) = i(k(m))$. A word W shall be *nondecreasing* if and only if each term of W is some i and W contains no k to the left of an i such that $i < k$. Thus 3 and $3\,3\,4$ are nondecreasing, but $3^{-1}\,4$ and $4\,3$ are not. A word W shall be *irredundant* if and only if either W is 1 or there is no i such that W contains i or more consecutive terms i.

Theorem 1. *Each π in S_n corresponds to one and only one word W which is irredundant and nondecreasing. Moreover, if π moves none of $i+1, \ldots, n$ then W contains none of $i+1, \ldots, n$.*

Note that there are only $n!$ distinct irredundant nondecreasing words. Hence if each π in S_n corresponds to at least one such word then none can correspond to more than one. Hence the uniqueness part of the theorem follows from the rest.

We prove this rest by induction. If π moves none of $2, \ldots, n$ then π corresponds to 1. Given any $i < n$ assume now as inductive hypothesis that the desired result holds for those π' in S_n which move none of $i+1, \ldots, n$. Consider any π in S_n which moves $i+1$ but none of $i+2, \ldots, n$. Then $\pi^{-1}(i+1) \leq i$. Let $k = (i+1) \cdots \pi^{-1}(i+1)$ and let $\pi' = \pi(i+1)^{-k}$. Since $(i+1)^{-k}$ maps $i+1$ into $\pi^{-1}(i+1)$, therefore π' does not move $i+1$. Also π' moves none of $i+2, \ldots, n$ since neither π nor $(i+1)^{-k}$ moves any of these. Hence by the inductive hypothesis π' corresponds to an irredundant nondecreasing word W' which contains none of

$i+1, \ldots, n$. If W' is $\mathbf{1}$ let W be the word $(i+1)^k$, i.e., the sequence consisting of k terms $i+1$. If W' is not $\mathbf{1}$ let W be the word $W'(i+1)^k$. In either case, W is irredundant, nondecreasing, and without terms $i+2, \ldots, n$. Moreover, since $\pi = \pi(i+1)^{-k}(i+1)^k$ therefore π corresponds to W. This concludes our proof (and directions for constructing W).

It follows from Theorem 1 that $\{\mathbf{1}, \ldots, n\}$ is a set of generators for S_n. In fact, as is well known and easy to see, $\{2, n\}$ is also a set of generators.

Henceforth e shall be the identity element of the group under consideration. Then equality (1) below holds for S_n. Now consider any i and k such that $i < k$. If $i = 1$ then $2(i+1) = 1 = kik^{-1}$, and if $i > 1$ then $2(i+1) = (2, \ldots, i+1) = k(i)k^{-1}$. It follows that each of the $\frac{1}{2}n(n-1)$ equalities (2) below hold for S_n.

(1) $\mathbf{1} = e$.

(2) $ki = 2(i+1)k$, if $k > i$.

A *presentation* of a group G consists of a set of generators for G and of a set E of equalities which involve (besides e) only these generators and which hold for G such that any equality which involves only these generators and which holds for G is a group-theoretic consequence of E. Various presentations of S_n are given in the book by Coxeter and Moser on *Generators and Relations for Discrete Groups* (Springer-Verlag, 1957). To these we now add another. Fairly generous regarding generators it is economical regarding equalities (or, rather, equality schemes).

Theorem 2. *The set* $\{\mathbf{1}, \ldots, n\}$ *and the equalities* (1) *and* (2) *together form a presentation of* S_n.

Let E be the set consisting of equality (1) and the $\frac{1}{2}n(n-1)$ equalities (2). We already saw that $\{\mathbf{1}, \ldots, n\}$ is a set of generators for S_n and that each equality belonging to E holds for S_n. It remains to show that each equality which involves only $\{\mathbf{1}, \ldots, n\}$ and which holds for S_n is a group-theoretic consequence of E. For this purpose it is convenient to change from S_n to an abstract group G_n for which $\{\mathbf{1}, \ldots, n\}$ and E form a presentation. Thus $\{\mathbf{1}, \ldots, n\}$ is from now on a generating set for G_n, and exactly those equalities involving only $\mathbf{1}, \ldots, n$ hold for G_n which are group-theoretic consequences of E. Since $\mathbf{1}, \ldots, n$ are elements of G_n there now corresponds to each word a unique element of G_n. It will be sufficient to prove that each element of G_n thus corresponds to some irredundant nondecreasing word. For by the uniqueness of this word for S_n this implies that G_n is isomorphic to S_n, so that $\{\mathbf{1}, \ldots, n\}$ and E also form a presentation of S_n.

One of our tasks will be to derive (3) below, i.e., to show that each of the n equalities (3) holds for G_n. Note that in contrast to (2) the length of (3) increases with k.

(3) $k^k = e$, for $1 \leqslant k \leqslant n$.

To derive (3), we shall now derive the following.

(4) $(i+1)k = 2ki$, if $k > i$.

(5) $(i+1)k^{i-1} = (2k)^{i-1}2$, if $k > i \geqslant 2$.

(6) $k^k=(2k)^{k-1}$, if $k\geqslant 2$.

(7) $(2k)^{k-1}=k(k-1)^{k-1}k^{-1}$, if $k\geqslant 2$.

To begin with, we derive $(3)_2$, the instance of (3) where $k=2$. We use $(3)_1=(1)$ and the instance of (2) where $k=2$ and $i=1$. One then obtains (4) from (2) and $(3)_2$. From (4) one obtains (5) by using induction on i. Specifically, if $2<i+1<k$ then by (4) and the inductive hypothesis respectively one obtains

$$((i+1)+1)kk^{i-1}=2k(i+1)k^{i-1}=2k(2k)^{i-1}2.$$

Now let $k\geqslant 2$. If $k=2$, then (6) is trivial. And if $k>2$ then (6) is obtained from (5) with $i=k-1$ by multiplication on the right by k. From the instance of (2) where $i=k-1$ one obtains $2k=k(k-1)k^{-1}$. One then obtains (7) by $(k(k-1)k^{-1})^{k-1}=k(k-1)^{k-1}k^{-1}$. Any instance of (3) can now be obtained from (1) and a sufficient number of instances of (7) and (6). This concludes our derivation of (3).

A $\{1,\ldots,k\}$-*word* shall be a word which contains no terms other than $1,\ldots,k$. We let $V\sim W$ if and only if the same element of G_n corresponds to V and W. We shall now prove the following assertions.

(8) If $1<i<k<n$, then there is some $\{1,\ldots,i+1\}$-word W, such that $((k+1)2)^{i-1}\sim W(k+1)^{i-1}$.

(9) If $i<k<n$, then there is some $\{1,\ldots,i+1\}$-word W, such that $(k+1)k^i\sim W(k+1)^{i+1}$.

(10) For each k and each $\{1,\ldots,k\}$-word V there is an irredundant nondecreasing $\{1,\ldots,k\}$-word W such that $V\sim W$.

To prove (8) we use induction on i. If $i=2$, we let $W=23$. Then by (2) (i.e., since (2) holds for G_n), $(k+1)2\sim W(k+1)$. Now let $i+1<k$ and assume that $((k+1)2)^{i-1}\sim U(k+1)^{i-1}$ for some $\{1,\ldots,i+1\}$-word U. By (2),

$$(k+1)2U\sim 23(k+1)U\sim 23V(k+1)$$

for some $\{1,\ldots,i+2\}$-word V. Hence, for $i+1$, $23V$ is a desired W.

To prove (9) let $i<k<n$. If $i=1$ then, by (2) the word 2 is a desired W. Now let $i>1$. By (2) and induction on i,

$$(k+1)k^i=(2(k+1))^i(k+1)=2((k+1)2)^{i-1}(k+1)^2.$$

By (8) there is some $\{1,\ldots,i+1\}$-word V such that $((k+1)2)^{i-1}\sim V(k+1)^{i-1}$. Hence $2V$ is a desired W.

To prove (10) we use induction on k. If $k\leqslant 2$, then by $(3)_1$ and $(3)_2$ there is a desired W. Now let $2\leqslant k<n$ and assume as inductive hypothesis that for each $\{1,\ldots,k\}$-word there is a desired W. Let U be any $\{1,\ldots,k\}$-word. Then either $U\sim U'$ or $U\sim k^i$ or $U\sim U'k^i$ for some $\{1,\ldots,k-1\}$-word U' and some $i<k$. By (2), (9), or (2) and (9) respectively there is some positive integer t and some $\{1,\ldots,k\}$-word U'' such that

$$(k+1)U\sim U''(k+1)^t.$$

By induction on the number of occurrences of $k+1$ in V it follows that for any $\{1, \ldots, k+1\}$-word V containing at least one occurrence of $k+1$ there is some positive integer t and some $\{1, \ldots, k\}$-word U'' such that $V \sim U''(k+1)^t$. By the inductive hypothesis and by (3), $U''(k+1)^t \sim W$ for some $\{1, \ldots, k+1\}$-word W which is irredundant and nondecreasing.

Now, by (3), for each word U there is some $\{1, \ldots, n\}$-word V such that $U \sim V$. Hence, by (10), for each word U there is an irredundant nondecreasing W such that $U \sim W$. Hence each element of G_n corresponds to some irredundant nondecreasing word. This concludes our proof of Theorem 2.

In conclusion we remark that (10) also holds for a different relation $\sim$. Let $1, \ldots, n$ be distinct letters of an alphabet, instead of elements of a group. Let (2)' be the rule which for each $k > i$ allows replacement of a (consecutive) part ki of a word W by $2(i+1)k$. Let (3)' be the rule which for each k allows deletion of a proper part k^k of a word and also replacement of an entire word k^k by the word 1. Let $V \sim W$ if and only if $V = W$ or V yields W by finitely many applications of rules (2)' and (3)'. (The new relation $\sim$ therefore is reflexive and transitive but not symmetric.) Now our proofs of (8), (9), (10) apply to the new relation $\sim$ if instead of (2) and (3) one uses (2)' and (3)'.

One may ask whether applications of rule (2)' alone always allow one to transform a $\{1, \ldots, n\}$-word V into a word W which is nondecreasing but which may be redundant. George M. Bergman, in a private communication, has shown that the answer is negative. He has characterized the $\{1, \ldots, 4\}$-words V which cannot be thus transformed. For example, 43423 and 44233 are among these.